REMARKS

Claims are being amended for better clarity. If the Examiner has questions regarding this case, the Examiner is invited to contact the Applicants' undersigned representative at the telephone number listed below.

Respectfully submitted,
Mark Moriconi et al.

Date: 7/26/02

By: _____

Eppa Hite, Reg. No. 30,266
Carr & Ferrell, *LLP*
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
Phone: (650) 812-3400
FAX: (650) 812-3444

VERSION MARKED UP TO SHOW CHANGES BEING MADE

1. (amended) A system for maintaining security in a distributed computing environment, comprising:

a policy manager for managing a security policy; and

an application guard for managing access to securable components as specified by the security policy;

wherein said securable components are separate and distinct from said security policy.

2. (amended) The system of claim 1[, wherein said policy manager] further compris[es]ing a management station for constructing and editing the security policy.

9. (amended) The system of claim 1, wherein said system [is scalable by] further [comprising] comprises a plurality of clients, said policy manager [further managing] manages and [distributing] distributes a customized local policy to each client, and each client includes at least one additional application guard [located on each client] for managing access to the securable components of that client as specified by each customized local policy.

18. (amended) A system for controlling user access in a distributed computing environment, comprising:

a global policy specifying access privileges of the user to securable components;

a policy manager located on a server for managing and distributing to a client a local client policy based on the global policy [to a client], and

an application guard located on the client for managing access to the securable components as specified by the local client policy.

19. (amended) The system of claim 18 further comprising at least one additional client, said policy manager further managing and distributing to each additional client a customized local policy based on the global policy [to each additional client], and comprising at least one additional application guard located on each additional client for managing access to the securable components as specified by the customized local policy.

48. (amended) A method for maintaining security in a distributed computing environment, comprising the steps of:

managing a policy by using a policy manager [by specifying] to specify access privileges of a user to securable components; and

distributing the policy to a client having an application guard[, whereby the application guard] which manages access to the securable components as specified by the policy.

51. (amended) A method for maintaining security on a client in a distributed computing environment, comprising the steps of:

using an application guard interface for [constructing and] issuing an authorization request for a user to gain access to securable components located on the client [using an application guard];

using the application guard to evaluate [evaluating] the authorization request [using the application guard to] and thereby determine if the authorization request is valid or invalid; and

allowing access to the user via the application guard if the evaluated authorization request was valid, and denying access to the user via the application guard if the authorization request was invalid.

53. (amended) A computer-readable medium comprising program instructions for maintaining security in a distributed computing environment by performing the steps of:

managing a policy by using a policy manager [by specifying] to specify access privileges of a user to securable components;

distributing the policy using the policy manager to a client having an application guard, whereby the application guard manages access to the securable components as specified by the policy; and

executing said policy manager with a processor to manage and distribute the policy.

59. (amended) A system [to protect computer systems against unauthorized access] for managing and enforcing complex security requirements to protect computer systems against unauthorized access in a distributed computer network comprising:

a policy manager located on a server for managing and distributing a policy to a client; and

an application guard located on the client, acting to grant or deny access to various components of the client, as specified by the policy.

65. (amended) The system of claim 59 wherein the server includes a non-volatile memory[, where] storing the policy manager [is located] that specifies the security requirements for applications and database objects;

said policy contains security rules that describe at least one constraint that constrains

which applications a particular user can access and

which objects within an application a user can access.

66. (amended) The system of claim 65 wherein the policy manager allows the administrator to choose whether the constraints are [effected] affected by any of

time,

geography, and

external events.

96. (amended) The system of claim 77 wherein conditions comprise constraints and the system [having] has at least facilities for defining constraints as expressions formed from operators including at least NOT, AND, and OR.

101. (amended) A system comprising a computer having a security policy that includes at least one or more components having at least a set of privileges that includes at least one privilege that is capable of at least:

being granted to [the] a user explicitly; and

being granted to a role which is granted to the user.

102. (amended) The system of claim 101 wherein:

the role is a named group of privileges containing at least one privilege that are granted to at least one user or to at least one other role; and

the at least one user granted [to] the role is a member of the role.

104. (amended) The system of claim 101 wherein roles are organized into a role hierarchy, where parent roles are granted to children roles such that:

if a parent role is granted a privilege, then the children roles are automatically granted the privilege; and

if a parent role is denied a privilege, then the children roles are automatically denied the privilege.

108. (amended) [The] A security system comprising a policy manager located on a computer system that includes at least:

a management console or station;

a database management system;

an audit facility; and

a distributor.

109. (amended) The system of claim 108 wherein the management station [further] comprises a Graphical User Interface (GUI) for users to create [creating] and customize [customizing] rules by system users.

111. (amended) The system of claim 108 wherein the management station includes an application guard to allow only authorized administrators to operate the management station based on at least a local administrative policy which provides a set of policy rules specifying which users are authorized to access the management station.

112. (amended) A security system comprising:

at least one application guard that is stored on a computer readable medium and that guards a protected application by preventing unauthorized transactional access to at least a portion of said application.

114. (amended) The security system of claim 113 further comprising a distributor capable of distributing the application guard [on] to clients located throughout an enterprise.

115. (amended) The system of claim 113 wherein the application guard is [integrated into] coupled to the application through an application programming interface (API) or authorization library that allows the application to request authorization services as needed through an application guard interface.

116. (amended) The system of claim 113 further comprising

an authorization engine that processes an authorization request;[.]

a checker that parses local client policy and stores the parsed local client policy in Random Access Memory (RAM); and

an evaluator that [determines whether the authorization request should be granted or denied by evaluating] evaluates the authorization request with the parsed local client policy in RAM to determine whether the authorization request should be granted or denied.

118. (amended) The system of claim 113 further comprising a logger where at least:

each authorization request is [then] recorded in an audit log; and

each authorization request made at a location remote from the logger is transmitted [to the logger] via a communication interface to the logger.

123. (amended) A method of using a security system comprising:

using a management station, including a communication interface, to create or modify a policy rule; and

distributing the policy rule to appropriate clients via [a] the communication interface [included in the management station].

124. (amended) The method of claim 123 further compris[es]ing reviewing and reconstructing the policy rules via a parser to make sure that the policy rules are syntactically and semantically correct according to a predefined policy language.

125. (amended) The method of claim 123 further compris[es]ing determining via a differ-program the changes that were made to optimize[d] the policy, and wherein the step of distributing then distributes only the changed policy rules or local client policy to the appropriate application guards, which enforce access control to local applications and data.

128. (amended) [The] A method of distributing at least one security policy rule comprising:

passing the policy rule through at least

a DataBase (DB) layer [(DB layer)] and

an Open DataBase Connectivity [layer] (ODBC) layer;

and

storing the policy rule as an enterprise policy.

135. (amended) The method of claim 133 wherein

if the administrator chooses to use the management station, then the step of entering includes using an edit function to enter the policy rules, and

if the administrator chooses to use the policy loader, then the step of entering includes

entering the policy rules into a file, and

passing the file to the policy loader.

136. (amended) A method of managing policy under management services in a management station comprising:

an authorized administrator logging into a policy manager;

the authorized administrator [chooses between] choosing either administrative mode to manage administrative policy or enterprise mode to manage enterprise policy;

presenting the administrator with menu options including

navigate tree,

analyze policy,

edit policy,

distribute policy,

view audit log [which is a security feature that allows an] to allow the administrator to view and track authorization requests that have occurred at an application guard connected to a system, and

exit.

137. (amended) The method of claim 136 wherein the menu option navigate tree provides a set of edit options for an administrator that include to

add,

delete, and

modify features; and

wherein the administrator is presented with a choice of features on a server and on a client.

138. (amended) The method of claim 136 wherein the features [that] to which the administrator [has the option] can apply the edit policy option[s] include

global users,

global roles,

directories,

local roles,

local users,

applications,

application guards, and

declarations.

139. (amended) The method of claim 136 wherein the menu option analyze policy allows an authorized user to analyze and view rules and policies within the enterprise policy.

140. (amended) The method of claim 136 wherein the [user] administrator is presented with [an] options

to search rules, and

to query policy.

144. (amended) The method of claim 143 wherein the features that may be edited include

a rule set,

access,

a privilege,

an object[s],

a[n] user

a role, and

an attribute.

146. (amended) The method of claim 136 wherein upon selecting the distribute policy option

a distributor optimizes enterprise policy;

a differ program computes a difference between a newly optimized policy and a formerly optimized policy;

the newly optimized policy is then published as optimized policy in DBMS;

[committing] only the changed portions of the newly optimized policy are committed to an appropriate application guard;

the application guard receives the changed portions of the newly optimized policy;

the application guard merges the received changed portions [newly optimized policy] into local client policy; and

the local client policy is activated to work with the application guard.

147. (amended) A method of granting client access authorization comprising:

using an application guard that includes at least

requesting access to a software securable component associated with an application protected by [an] the application guard, wherein the application guard constructs and issues an authorization request, and

evaluating the authorization request via the application guard according to its local client policy to determine whether to allow or deny the authorization request; and

an audit records the authorization request in an audit log;

wherein

if there is an error in the authorization request, or if the request is not valid, then [the user] access is denied [access];

if the authorization request is valid, then a determination is made whether access should be granted, and

if the evaluated authorization request does not deny access [for the user], then access is allowed, and

if the evaluated authorization request denies access [for the user], then access is denied.

148. (amended) The method of claim 147 wherein evaluating the authorization request includes an evaluator searching deny rules in a local policy, and

if the evaluator finds a deny rule, then an evaluation is performed on any constraints on the deny rule,

if the evaluation finds a presently valid constraint on the deny rule, then access is denied, and

if the evaluation finds that all constraints on the deny rule are not presently valid, then a search for a grant rule is performed;

and

if no deny rules are found, then a search for a grant rule is performed;

wherein after a search for a grant rule

if no grant rule is found that would allow access for the user, then access is denied, and

if a grant rule is found, then an evaluation is performed on any constraints in the grant rule[s] wherein

if the evaluated constraint is presently valid, then access is allowed, and

if the evaluated constraint is not presently valid, then access is denied.

150. (amended) A method for providing a security system, comprising:

providing at least one application guard that is storable on a computer readable medium and guards a protected application by preventing unauthorized transactional access to at least a component associated with the application.

151. (amended) A method for updating a security system, comprising:

updating a set of policy rules containing at least one policy rule in a central location;

generating changes to the set of policy rules resulting from the updating step; and

distributing the changes [to the set of policy rules].

154. (amended) A method for establishing a security system, comprising:

establishing a set of policy rules containing at least one policy rule in a central location; and

distributing the set of policy rules for enforcement.